PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 15.10.2001

# E T U O I K E U S T O D I S T U S
# P R I O R I T Y  D O C U M E N T

| | |
|---|---|
| Hakija<br>Applicant | **Sonera Oy**<br>**Helsinki** |
| Patenttihakemus nro<br>Patent application no | **990846** |
| Tekemispäivä<br>Filing date | **15.04.1999** |
| Kansainvälinen luokka<br>International class | **H04Q 7/32** |

Keksinnön nimitys
Title of invention

**"Tilaajaidentiteettimoduulin hallinta"**

Hakijan nimi on hakemusdiaariin **05.03.2000** tehdyn nimenmuutoksen jälkeen **Sonera Oyj**.

The application has according to an entry made in the register of patent applications on **05.03.2000** with the name changed into **Sonera Oyj**.

Hakemus on hakemusdiaariin **30.09.2001** tehdyn merkinnän mukaan siirtynyt **Sonera Smarttrust Oy**:lle, **Helsinki**.

The application has according to an entry made in the register of patent applications on **30.09.2001** been assigned to **Sonera Smarttrust Oy, Helsinki**.

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

*Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1782/1995 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.*

*The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1782/1995 concerning the chargeable services of the National Board of Patents and Registration of Finland.*

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

# TILAAJAIDENTITEETTIMODUULIN HALLINTA

## TEKNIIKAN ALA

Keksintö kohdistuu tietoliikennejärjestelmiin. Erityisesti keksinnön kohteena on menetelmä tilaajaidentiteettimoduulin hallitsemiseksi ja tilaajaidentiteettimoduuli, joka käsittää välineet sen muistialueiden hallitsemiseksi.

Keksinnön kohteena on menetelmä tilaajaidentiteettimoduulille tallennettujen varmenteiden hallitsemiseksi. Menetelmässä vastaanotetaan tilaajaidentiteettimoduulille varmenne, ja tallennetaan mainitusta varmenteesta tietoa tilaajaidentiteettimoduulille.

## KEKSINNÖN TAUSTAA

Matkaviestinverkot, esimerkiksi GSM-verkot (GSM, Global System for Mobile communications) ovat viime aikoina saavuttaneet suuren suosion. Matkaviestinverkkoihin liittyvät lisäpalvelut ovat lisääntyneet vastaavasti yhä kiihtyvällä vauhdilla. Sovellusalueet voivat olla mitä erilaisempia. Matkapuhelinta voidaan käyttää muun muassa pienten ostosten, esimerkiksi virvoitusjuoma- ja autopesuautomaattien maksuvälineenä. Arkipäiväisiä toimintoja, kuten maksutoiminteita, pankkipalveluita ja niin edelleen, on lisätty ja tullaan vastaisuudessakin lisäämään nykyisten matkaviestimien palveluvalmiuteen. Seuraavan sukupolven matkaviestimet tulevat olemaan edellisiään huomattavasti palvelutasoltaan ja tiedonsiirtokapasiteetiltaan kehittyneempiä.

Nykyisin on tunnettua käyttää digitaalista GSM-matkaviestintä kaupallisiin transaktioihin, kuten laskun tai maksun maksamiseen sähköisesti. Patenttijulkaisusta US 5,221,838 tunnetaan laite, jota voidaan käyttää maksamiseen. Julkaisussa on kuvattu sähköinen maksujärjestelmä, jossa maksupäätteenä käytetään lan-

gattomaan ja/tai langalliseen tiedonsiirtoon kykenevää päätelaitetta. Julkaisun mukaiseen päätelaitteeseen kuuluu kortinlukija, näppäimistö, ja viivakoodin lukija tietojen syöttämiseksi ja näyttö maksuinformaation esittämiseksi.

Patenttijulkaisusta WO 94/11849 tunnetaan menetelmä tietoliikennepalveluiden käyttämiseksi ja maksuliikenteen suorittamiseksi matkapuhelinjärjestelmällä. Julkaisussa kuvataan järjestelmä, johon kuuluu päätelaite, joka on yhteydessä televerkon kautta palveluntarjoajan keskustietokoneeseen, joka sisältää palveluntarjoajan maksujärjestelmän. Matkapuhelinverkon päätelaitteeseen eli matkaviestimeen voidaan lisätä tilaajan tunnistusyksikkö, joka käsittää tilaajatiedot tilaajan tunnistamiseksi ja teleliikenteen salaamiseksi. Tiedot voidaan lukea päätelaitteeseen käytettäväksi matkaviestimissä. Esimerkkinä julkaisussa mainitaan GSM-järjestelmä, jossa käytetään tilaajaidentiteettimoduulia tai SIM-korttia (Subscriber Identity Module, SIM) tilaajan tunnistusyksikkönä.

Julkaisun WO 94/11849 mukaisessa järjestelmässä matkaviestin on yhteydessä matkapuhelinverkon tukiasemaan. Julkaisun mukaan yhteys muodostetaan tukiasemasta edelleen maksujärjestelmään ja maksettava määrä samaten kuin tilaajan tunnistamiseen tarvittava data välitetään maksujärjestelmään. Julkaisussa kuvatussa pankkipalvelussa asiakas asettaa pankin palvelukortin, joka sisältää SIM-yksikön, GSM-verkon päätelaitteeseen. Puhelinperustaisessa pankkipalvelussa päätelaite voi olla standardin mukainen GSM-matkaviestin. Julkaisussa kuvatulla menetelmällä voidaan käyttää langatonta tietoliikenneyhteyttä maksujen ja/tai laskujen tai muiden vastaavien pankkipalvelujen tai kassapalvelujen toteuttamiseen.

Digitaalisella allekirjoituksella, jota pidetään yleisenä vaatimustasona sähköisessä maksamisessa, varmistetaan välitettävän aineiston eheys ja lähettä-

jän alkuperä. Digitaalinen allekirjoitus muodostetaan salaamalla välitettävästä aineistosta laskettu tiiviste lähettäjän salaisella avaimella. Koska kukaan muu ei tunne lähettäjän salaista avainta, voi vastaanottaja purkaessaan salauksen lähettäjän julkista avainta käyttäen varmistua siitä, että aineisto on muuttumaton ja lähettäjän tuntemallaan salaisella avaimellaan muodostama. Eräs esimerkki digitaalisessa allekirjoituksessa käytettävästä algoritmista on RSA-salausalgoritmi, joka on julkisen ja salaisen avaimen salausjärjestelmä ja jota käytetään myös viestien salaamiseen.

Jotta voidaan käyttää yhtenäisiä menettelyjä kaupan tai muun sopimuksen osapuolten luotettavaan tunnistamiseen tietoliikenneverkolla, tarvitaan sähköinen identiteetti ja keinot identiteetin todistamiseen ja toteamiseen. Tällainen sähköinen identiteetti voi olla myös ns. verkkoidentiteetti (Net-ID, Network Identity). Sähköinen identiteetti perustuu älykortilla, tilaajaidentiteettimoduulilla tai vastaavalla oleviin henkilötietoihin ja avainpariin, salaiseen avaimeen ja julkiseen avaimeen, joka on tallennettu varmennehakemistoon luotetulle kolmannelle osapuolelle. Tällaisella tekniikalla voidaan toteuttaa viranomaisille ja muille palveluntarjoajille riittävän turvallisesti mm. osapuolten tunnistus, sähköinen allekirjoitus, salakirjoittaminen ja asioinnin kiistämättömyys.

Tässä hakemuksessa identiteetillä tarkoitetaan henkilöön liitettävää yksilöivää tietoa, jonka avulla henkilö voidaan tunnistaa. Samaten identiteetillä voidaan tarkoittaa sovellusta tai palvelua tarkoittavaa yksilöivää tietoa, jonka avulla sovellus tai palvelu voidaan tunnistaa.

Julkisen avaimen menetelmässä käyttäjä säilyttää salaisen avaimen ainoastaan omassa hallussaan ja julkinen avain on yleisesti saatavilla. Ei riitä,

että julkinen avain talletetaan sellaisenaan esimerkiksi sähköpostin hakemistoon, koska joku saattaisi väärentää sen ja esiintyä sen jälkeen avaimen oikean haltijan nimissä. Sen sijaan tarvitaan varmennuspalvelua ja varmennetta, joka on luotetun tahon (varmentaja) todistus siitä, että nimi, henkilön tunnus ja julkinen avain kuuluvat samalle henkilölle. Varmenne on yleensä henkilön julkisesta avaimesta, nimestä, henkilötunnuksesta ym. tiedoista muodostuva kokonaisuus, jonka varmentaja allekirjoittaa omalla salaisella avaimellaan.

Kun sähköisesti allekirjoitetun sanoman vastaanottaja haluaa varmistua sanoman aitoudesta, hänen on ensin hankittava käyttöönsä lähettäjän varmenne, josta hän saa tämän julkisen avaimen ja nimen. Sen jälkeen hänen on todennettava varmenteen oikeellisuus. Tätä varten hänen on mahdollisesti hankittava käyttöönsä vielä muita varmenteita (varmenneketju), joita on käytetty kyseisen varmenteen varmentamiseen.

Jos varmenne on aito, vastaanottaja todentaa sanoman allekirjoituksen lähettäjän varmenteessa saamallaan julkisella avaimella. Jos allekirjoitus läpäisee testin, lähettäjä on varmenteen osoittama henkilö. Varmenteiden käyttöön liittyy myös sulkulista, jolle merkitään käytöstä poistetut varmenteet. Varmenteita ja sulkulistaa varten tarvitaan hakemistopalvelut.

Kun tilaajaidentiteettimoduulille tallennetaan erilaisia sovelluksia, joita käytetään sähköiseen maksamiseen, kaupankäyntiin, pankkiasioiden hoitamiseen yms., tallennetaan samalla näiden sovellusten käyttämien palveluntarjoajien, kuten kaupan, pankin ja muiden sähköisiä palveluita tarjoavien organisaatioiden palvelussa käyttämät julkiset avaimet. Julkisia avaimia voidaan myös tallentaa myöhemmin riippuen tilaajaidentiteettimoduulin käyttäjän käyttämistä palveluista. Tällöin tilaajaidentiteettimoduulin käyttäjän ei erikseen tarvitse hakea varmennetta jokaista trans-

aktiota varten, vaan varmenne on valmiina tilaajaidentiteettimoduulilla.

Tällä hetkellä varmenteen kokoa ei voida rajoittaa. Mitä pidempi varmennusketju varmenteen muodostamiseen on syntynyt, sitä enemmän tietoa varmenne sisältää. Pitkät varmennusketjut ja sitä myöden paljon muistia kuluttavat varmenteet ovat ongelmallisia nykyisille tilaajaidentiteettimoduuleille, koska tilaajaidentiteettimoduulin muistialue on rajattu. Tämä rajoittaa merkittävästi tilaajaidentiteettimoduulin käyttämistä erilaisiin palveluihin, joilla on eri varmenne. Näin ollen olisikin tärkeää, että varmenteen kokoa voitaisiin rajoittaa ja siten saada useampia varmenteita mahtumaan yhdelle tilaajaidentiteettimoduulille. Yksi palvelusovellus tilaajaidentiteettimoduulilla voi käyttää useita eri varmenteita asioidessaan käyttäjän puolesta eri palveluntarjoajien palveluissa. Näin ollen tilaajaidentiteettimoduulilla käytettävien eri palveluiden määrää rajoittaa miltei yksinomaan varmenteiden koko.

**KEKSINNÖN TARKOITUS**

Esillä olevan keksinnön tarkoituksena on poistaa tai ainakin merkittävästi lieventää edellä esitettyjä ongelmia. Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin menetelmä ja tilaajaidentiteettimoduuli, joilla varmenteen koko pystytään määräämään tai ainakin kokoa voidaan supistaa, jolloin matkaviestinympäristössä käytettävien varmenteiden lukumäärää yhdellä tilaajaidentiteettimoduulilla voidaan kasvattaa.

Lisäksi keksinnön tarkoituksena on tuoda esiin menetelmä, jota käyttäen tilaajaidentiteettimoduulille voidaan tallentaa aikaisempaa useampia varmenteita katkaisematta luottamusketjua varmenneketjussa.

Esillä olevan keksinnön tunnusomaisten piirteiden osalta viitataan oheisiin patenttivaatimuksiin.

**KEKSINNÖN YHTEENVETO**

Keksinnön mukaisen ratkaisun toiminnan pääperiaatteena on tallentaa tilaajaidentiteettimoduulille tallennettavat varmenteet siten, että niistä poistetaan varmenneketjun sisältämät varmenteet. Tämä voidaan tehdä, jos tilaajaidentiteettimoduulille tallennetulla korttivarmenteella pystytään todentamaan oikeaksi tilaajaidentiteettimoduulille vastaanotettu varmenne. Kun varmenneketju on poistettu, jäljelle jäävä julkinen avain ja siihen liittyvä identiteetti tallennetaan suojatulle muistialueelle, jonne ei muilla sovelluksilla kuin korttivarmenteen käyttämällä sovelluksella ole pääsyä. Aina kun tilaajaidentiteettimoduulilla oleva palvelusovellus haluaa käyttää kortille tallennettua varmennetta, se pyytää sitä suojatulta muistialueelta korttivarmenteen käyttämältä sovellukselta. Korttivarmenteen käyttämä sovellus varmentaa suojatulta muistialueelta luetun varmenteen ja kun käyttäjä luottaa korttivarmenteen antajaan, voi käyttäjä luottaa myös kortilta luettuun varmenteeseen.

Keksinnön perusajatus voidaan kiteyttää vielä seuraavasti. Jokin toiminnallinen yksikkö on jaettu kahteen osaan A ja B sekä ehtoon C. Toiminnallinen yksikkö voi olla tilaajaidentiteettimoduulin muistilaite tai muisti ja ehto C voi olla suodatin tai algoritmi, joka hallitsee muistialuetta. Osan A toiminta on tunnettu, avoin muistialue, ja sen toiminnallisuuksiin voidaan vaikuttaa tunnetuilla ohjeilla, tilaajaidentiteettimoduulin käyttöjärjestelmällä. Osa B voi toimia samalla tavalla kuin osa A, mutta B:n toiminnallisuuksia voi käyttää vain ehdot C tunteva. Tässä tapauksessa ehdon C tuntee vain korttivarmenteen antava varmenneviranomainen D ja kortilla oleva suodatin tai algoritmi, joka hallitsee suojattua muistialuetta.

Kun tilaajaidentiteettimoduulille tallennetaan uusi varmenne, pyytää uuden varmenteen luovuttaja varmenneviranomaiselta D varmenteensa tallennusta tilaajaidentiteettimoduulille. Varmenneviranomainen D autentikoi toiselta varmenneviranomaiselta E saadun uuden varmenteen ja poimii varmenteesta vain ne komponentit F, jotka välttämättä tarvitaan tilaajaidentiteettimoduulille tallennettavaksi.

Varmenneviranomainen D muodostaa E:n antamasta uudesta varmenteesta ja poimimistaan komponenteista F oman varmenteensa G. Varmenteesta G arkistoidaan hakemistoon tarvittavat tiedot, jotta voidaan lukea, mistä varmenteesta aineisto F on luotu ja todeta, että aineisto on varmenneviranomaisen D varmentama.

Koska vain varmenneviranomainen D tuntee ehdot, miten F sijoitetaan suojatulle alueelle B, voidaan F tulkita varmenteeksi, joka ei ole julkinen ja johon voidaan luottaa.

Keksinnön mukaisessa menetelmässä tilaajaidentiteettimoduulille tallennettujen varmenteiden hallitsemiseksi vastaanotetaan tilaajaidentiteettimoduulille varmenne ja tallennetaan mainitusta varmenteesta tietoa mainitulle tilaajaidentiteettimoduulille. Tilaajaidentiteettimoduuli käsittää tietojenkäsittelylaitteen muistilaitteen, joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen, muistilaitteelle tallennetun korttivarmenteen, sovelluksen, joka käyttää tilaajaidentiteettimoduulille tallennettuja varmenteita ja tiedonsiirtolaitteen, joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen ja johon on järjestetty liityntärajapinta tiedon siirtämiseksi ulkoisen laitteen, kuten matkaviestimen, ja tilaajaidentiteettimoduulin välillä.

Keksinnön mukaisesti todennetaan mainittu varmenne oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista ja suodatetaan mainitusta oikeaksi todennetusta varmenteesta sen sisältämä varmen-

neketju. Ennen suodatusta voidaan vielä erikseen tarvittaessa varmentaa jokainen varmenneketjun allekirjoitus ja varmenne. Suodatuksen jälkeen varmenteesta jää tallennettavaksi sen sisältämä julkinen avain ja siihen liittyvä identiteetti, mutta myös muita tietoja voidaan tallentaa. Tällä tavalla voidaan merkittäväsiti pienentää varmenteen käyttämän muistin määrää. Kun varmennetta halutaan käyttää, on se ensin varmennettava korttivarmenteella.

Keksinnön eräässä sovelluksessa hylätään mainittu varmenne, jos se todennetaan epäluotettavaksi ennen sen tallentamista tai ennen sen käyttöä. Kun vielä käytetään luotettavia välineitä ja ohjelmistoja, voidaan täten varmenteisiin ja niillä tehtyihin transaktioihin luottaa. Kuitenkin tässä huomautamme, että jos korttivarmenne hylätään, se ei välttämättä tarkoita sitä, että varmennetta ei voisi käyttää jokin kortilla oleva sovellus. Tällöin, jos jokin sovellus varmenteen tunnistaa, se voidaan tallentaa tilaajaidentiteettimoduulille. Ainoa ero suodatettuun varmenteeseen on, että varmenne tallennetaan kokonaisena suodattamatta siitä mitään pois.

Keksinnön mukainen tilaajaidentiteettimoduuli varmenteiden hallitsemiseksi käsittää edellä mainitut komponentit. Lisäksi tilaajaidentiteettimoduuli käsittää välineet varmenteen vastaanottamiseksi tilaajaidentiteettimoduulille ja välineet mainitun varmenteen sisältämän tiedon tallentamiseksi muistilaitteelle.

Keksinnön mukaisesti tilaajaidentiteettimoduuli käsittää välineet varmenteen todentamiseksi oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista ja välineet oikeaksi todennetun varmenteen sisältämän varmennusketjun suodattamiseksi varmenteesta. Edelleen tilaajaidentiteettimoduuli käsittää välineet varmenteen varmentamiseksi korttivarmenteella ennen sen käyttämistä.

Keksinnön eräässä sovelluksessa tilaajaidentiteettimoduuli edelleen käsittää välineet varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen tallentamista, ja välineet varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen käyttämistä. Edelleen tilaajaidentiteettimoduuli voi käsittää välineet jokaisen mainittuun varmenteeseen sisältyvän allekirjoituksen todentamiseksi ennen suodatusta.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että varmenteita voidaan sijoittaa rajoitetulle muistille entistä enemmän. Erityisesti keksinnön ansiosta tilaajaidentiteettimoduulille tai älykortille voidaan tallentaa useampi varmenne.

Edelleen keksinnön etuna tunnettuun tekniikkaan verrattuna on, että tilaajaidentiteettimoduulin päivitys uusilla varmenteilla ja sovelluksilla voidaan varmentaa keksinnön mukaisella varmistusmenetelmällä korttivarmennetta käyttäen.

**KUVALUETTELO**

Seuraavaksi keksintöä selostetaan suoritusesimerkkien avulla viittaamalla oheiseen piirustukseen, jossa

kuvio 1 esittää kaaviomaisesti erästä esillä olevan keksinnön mukaista tilaajaidentiteettimoduulia,

kuvio 2 esittää kaaviomaisesti erästä keksinnön mukaista menetelmää varmenteen tallentamiseksi tilaajaidentiteettimoduulille, ja

kuvio 3 esittää kaaviomaisesti sanomarakennetta, jota voidaan käyttää esillä olevan keksinnön mukaisessa menetelmässä.

Kuviossa 1 esitettyyn tilaajaidentiteettimoduuliin (Subscriber Identity Module, SIM) kuuluu tietojenkäsittelylaite 1, kuten prosessori, mikrokontrolleri tai vastaava, muistilaite 2, joka on yhdistetty tietojenkäsittelylaitteeseen 1 ja tiedonsiirtolaite 3,

joka on yhdistetty tietojenkäsittelylaitteeseen 1. Lisäksi tilaajaidentiteettimoduuliin SIM on järjestetty liityntärajapinta RP tiedon siirtämiseksi ulkoisen laitteen, kuten GSM-matkaviestimen ja tilaajaidentiteettimoduulin välillä.

Lisäksi kuviossa 1 esitettyyn tilaajaidentiteettimoduuliin kuuluu tai sinne on tallennettu sovellus APP, joka käyttää tilaajaidentiteettimoduulille tallennettuja varmenteita ollessaan yhteydessä palveluntarjoajan palveluihin. Edelleen tilaajaidentiteettimoduulille on järjestetty välineet 4 varmenteiden vastaanottamiseksi ja välineet 5 tietojen tallentamiseksi varmenteesta muistilaitteelle 2. Lisäksi tilaajaidentiteettimoduulilla on välineet 6 vastaanotetun varmenteen todentamiseksi oikeaksi mainitulla korttivarmenteella (CACert) ja välineet 7 oikeaksi todennetun varmenteen sisältämän varmenneketjun suodattamiseksi varmenteesta ennen varmenteen tallentamista.

Edelleen kuviossa 1 esitetty tilaajaidentiteettimoduuli käsittää välineet 8 tilaajaidentiteettimoduulille tallennetun varmenteen Mcert_1 varmentamiseksi korttivarmenteella CA_Cert ennen sen käyttämistä. Lisäksi tilaajaidentiteettimoduulilla on välineet 9 varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen tallentamista ja välineet 10 varmenteen hylkäämiseksi, jos varmenne todennetaan epäluotettavaksi ennen käyttöä. Edelleen tilaajaidentiteettimoduuli käsittää välineet 11 jokaiseen mainittuun varmenteeseen sisältyvän allekirjoituksen todentamiseksi ennen allekirjoituksen poissuodattamista.

Lisäksi kuviossa 1 on esitetty yllä olevaan esimerkkiin viitaten alueet A ja B, jotka siis ovat suojaamaton muistialue A ja suojattu muistialue B. Suojatulle muistialueella tallennetaan ainakin korttivarmenne Card_CA, joka käsittää korttivarmenteen antajan sähköisen tai verkkoidentiteetin, lyhyen nimikuvauksen varmenneviranomaisesta, varmenteen tyypin, esi-

merkiksi RSA, julkisen salausavaimen, julkisen allekirjoitusavaimen, varmenteen statuksen eli tiedon siitä, onko varmenne aktiivinen vai passiivinen ja lyhytsanomakeskuksen numero, joka viittaa varmenteen antajaan. Lisäksi suojatulle muistialueelle on tallennettu käyttäjän oma varmenne, joka voi esimerkinomaisesti käsittää muuten samat tiedot kuin edellä kuvattiin korttivarmenteen yhteydessä paitsi julkinen salausavain ja julkinen allekirjoitusavain korvataan salaisella salausavaimella ja salaisella allekirjoitusavaimella, vastaavasti. Käyttäjän varmenteeseen viitataan tässä esimerkissä termillä Mcert_1:llä. Lisäksi suojatulle muistialueelle B voidaan tallentaa palveluntarjoajien varmenteita, joista siis on suodatettu pois varmenneallekirjoitukset niiden varaaman muistialueen pienentämiseksi. Näihin varmenteisiin viitataan merkinnällä MCert_n. Myös näissä varmenteissa on edullisesti samat tiedot kuin korttivarmenteessa.

Seuraavaksi esitetään viitaten kuvioon 2 eräs edullinen toimintamalli vastaanotettaessa varmenne tilaajaidentiteettimoduulille. Ensin varmenne vastaanotetaan tilaajaidentiteettimoduulille, lohko 20. Varmenne on korttivarmenteen antajan varmentama ja tämä tarkistetaan lohkossa 21. Jos havaitaan, että vastaanotettua varmennetta ei voida todentaa oikeaksi kortille tallennetulla korttivarmenteellakaan Card_CA, hylätään varmenne. Vaihtoehtoisesti proseduuri voitaisiin lopettaa tähän, mutta tässä esimerkissä voidaan pyytää varmenteen uudelleenlähetystä, lohko 25 ja sen jälkeen tarkistaa varmenne uudelleen. Tämä voidaan toistaa esimerkiksi kolme kertaa ja jos kolmannellakaan kerralla varmennetta ei todenneta oikeaksi, lopetetaan proseduuri.

Jos lohkossa 21 varmenne todennettiin oikeaksi, suodatetaan varmenteesta koko varmenneketju, jolloin jäljelle jää julkinen avain ja siihen liittyvä

identiteetti ja mahdollisesti jotain muuta tietoa, lohko 23. Tämän jälkeen suodatettu varmenne tallennetaan, lohko 24, varmennetulle suodatetulle alueelle B-tilaajaidentiteettimoduulilla.

Seuraavaksi esitetään kuvioon 3 viitaten edullisia sanomarakenteita, joita voidaan käyttää keksinnön mukaisten varmenteiden lähettämiseksi ilmarajapinnan kautta tilaajaidentiteettimoduulille. Tässä esimerkissä oletetaan, että käytettävä sanomatyyppi on lyhtysanomaviesti (Short Message Service, SMS), mutta kuten ammattimiehelle on selvää, myös muita sanomamuotoja voitaisiin käyttää. Tässä esimerkissä varmenteen lähettämiseen käytetään kolmea lyhytsanomaviestiä, joissa on kuvion 3 mukainen sisältö.

Ensimmäinen lähetettävä sanoma on salaamaton (Non-encrypted SMS-message #1), jossa on kaksi kenttää. PublicKeyMod on julkinen verifiointi tai salausavain. Lisäksi viestissä on viestin järjestysnumero, MsgNumber. Tämän viestin pituus on yhteensä 1033 bittiä, jossa julkinen avain on 1025 bittiä ja sanomanumero 8 bittiä. Toisessa viestissä, Downloaded Data in message #2, on viisi kenttää. S3HDT Kuvaa viestin tyyppiä, ReceiverID vastaanottajan identiteettiä, SenderID lähettäjän identiteettiä, jossa identiteetti voi olla esimerkiksi verkkoidentiteettitunnus, S3AP on osoitin, joka viittaa sovellukseen, joka kyseistä varmennetta käyttää, ja lisäksi viestiin kuuluu RSA-lohko, ENCDATA, joka on oletusarvoisesti allekirjoitettu ja salattu. Tämän viestin koko on 1120 bittiä.

Allekirjoitettu ja salattu data, ENCDATA, viestissä käsittää viisi kenttää, joista ensimmäisessä on RSA:n eniten merkitsevä bitti RSA_MSB, aloituskenttä, Start, satunnaisluvun juuri, Random, siirretty data SP_data ja Hash-tarkiste SP_data-kentän sisällöstä. Tarkisteella tarkistetaan tiedon eheys ja varmistetaan ettei tieto ole muuttunut lähetyksen aikana.

Edelleen SP_data viestissä #2 käsittää kahdeksan kenttää, joista ensimmäinen, NID, viittaa korttivarmenteen identiteettiin, Short Name viittaa avaimenhaltijan nimeen, Key Usage, avaimen käyttötarkoitukseen, KeyHash on tarkisteeseen viestistä numero 1, MCertHash tarkisteeseen varmenteesta, ja viestin numeron, MSG Number. Lopuksi lähetetään kolmas viesti, joka edelleen on viestin 2 ENCDATA SP_data-kenttää, jossa edelleen on osoitin korttivarmenteen antajan avainpariin NID, julkisen avaimen eksponentti, PublicKeyE ja viestin järjestysnumero MsgNumber. Huomautamme vielä, että edellä olevaa kuvausta edullisista sanomarakenteista ei ole tarkoitettu rajoittavaksi, vaan erääksi esimerkiksi keksinnön käytöstä. Kun todennetaan kortille tai tilaajaidentiteettimoduulille vastaanotettua varmennetta oikeaksi, käytetään yllä kuvattuja Hash-tarkisteita. Niiden avulla voidaan vakuuttua siitä, että vastaanotettu varmenne on tietyn ennalta määrätyn varmenneviranomaisen tai varmenteenantajan allekirjoittama ja varmentama. Kun varmenne on todettu oikeaksi, voidaan siitä poimia tai suodattaa julkinen avain ja siihen liittyvä identiteetti tallennettavaksi suodatetulle alueella B.

Esillä olevaa keksintöä ei rajata tässä esitettyihin esimerkkeihin, vaan monet muunnokset ovat mahdollisia pysyttäessä oheisten patenttivaatimusten määrittelemän suojapiirin rajoissa.

**PATENTTIVAATIMUKSET**

1. Menetelmä tilaajaidentiteettimoduulille tallennettujen varmenteiden hallitsemiseksi, joka tilaajaidentiteettimoduuli käsittää:

- tietojenkäsittelylaitteen (1),
- muistilaitteen (2), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1)
- muistilaitteelle tallennetun korttivarmenteen (CA),
- sovelluksen (APP), joka käyttää tilaajaidentiteettimoduulille tallennettuja varmenteita ja
- tiedonsiirtolaitteen (3), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1) ja johon on järjestetty liityntärajapinta (RP) tiedon siirtämiseksi ulkoisen laitteen ja tilaajaidentiteettimoduulin välillä, joka menetelmä käsittää seuraavat vaiheet:
- vastaanotetaan tilaajaidentiteettimoduulille varmenne, ja
- tallennetaan mainitusta varmenteesta tietoa mainitulle muistilaitteelle, t u n n e t t u siitä, että menetelmä edelleen käsittää seuraavat vaiheet:
- todennetaan mainittu varmenne oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista, ja
- suodatetaan mainitusta oikeaksi todennetusta varmenteesta sen sisältämä varmenneketju.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että varmennetaan mainittu varmenne korttivarmenteella ennen sen käyttämistä.

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tallennetaan mainitusta varmenteesta sen sisältämä julkinen avain ja siihen liittyvä identiteetti.

4. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että hylätään mainittu varmenne,

jos se todennetaan epäluotettavaksi ennen sen tallentamista.

5. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että hylätään mainittu varmenne, jos se todennetaan epäluotettavaksi ennen sen käyttöä.

6. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että suodatusvaiheessa:

todennetaan jokainen mainittuun varmenteeseen sisältyvä allekirjoitus,

ja suodatetaan mainitusta varmenteesta vain oikeaksi todennetut allekirjoitukset.

7. Tilaajaidentiteettimoduuli varmenteiden hallitsemiseksi, joka tilaajaidentiteettimoduuli käsittää:

- tietojenkäsittelylaitteen (1),
- muistilaitteen (2), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1)
- muistilaitteelle tallennetun korttivarmenteen (CA),
- sovelluksen (APP), joka käyttää varmenteita,
- tiedonsiirtolaitteen (3), joka on yhdistetty mainittuun tietojenkäsittelylaitteeseen (1) ja johon on järjestetty liityntärajapinta (RP) tiedon siirtämiseksi ulkoisen laitteen ja tilaajaidentiteettimoduulin välillä, joka menetelmä käsittää seuraavat vaiheet,
- välineet (4) varmenteen vastaanottamiseksi tilaajaidentiteettimoduulille, ja
- välineet (5) mainitun varmenteen sisältämän tiedon tallentamiseksi mainitulle muistilaitteelle, t u n n e t t u siitä, että tilaajaidentiteettimoduuli edelleen käsittää:
- välineet (6) mainitun varmenteen todentamiseksi oikeaksi mainitulla korttivarmenteella ennen varmenteen tallentamista, ja

- välineet (8) mainitun oikeaksi todennetun varmenteen sisältämän varmennusketjun suodattamiseksi varmenteesta.

8. Patenttivaatimuksen 7 mukainen tilaajaidentiteettimoduuli, t u n n e t t u siitä, että tilaajaidentiteettimoduuli edelleen käsittää välineet (8) mainitun varmenteen varmentamiseksi korttivarmenteella ennen sen käyttämistä.

9. Patenttivaatimuksen 7 mukainen tilaajaidentiteettimoduuli, t u n n e t t u siitä, että tilaajaidentiteettimoduuli edelleen käsittää välineet (9) mainitun varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen tallentamista.

10. Patenttivaatimuksen 7 mukainen tilaajaidentiteettimoduuli, t u n n e t t u siitä, että tilaajaidentiteettimoduuli edelleen käsittää välineet (10) mainitun varmenteen hylkäämiseksi, jos se todennetaan epäluotettavaksi ennen sen käyttämistä.

11. Patenttivaatimuksen 7 mukainen tilaajaidentiteettimoduuli, t u n n e t t u siitä, että tilaajaidentiteettimoduuli edelleen käsittää välineet (11) jokaisen mainittuun varmenteeseen sisältyvän allekirjoituksen todentamiseksi ennen suodatusta.

**(57) TIIVISTELMÄ**

Keksinnön kohteena on menetelmä tilaajaidentiteettimoduulille tallennettujen varmenteiden hallitsemiseksi. Menetelmässä vastaanotetaan tilaajaidentiteettimoduulille varmenne, ja tallennetaan mainitusta varmenteesta tietoa tilaajaidentiteettimoduulille. Keksinnön ansiosta tilaajaidentiteettimoduulille voidaan tallentaa aiempaa useampia varmenteita.

(Fig. 1)

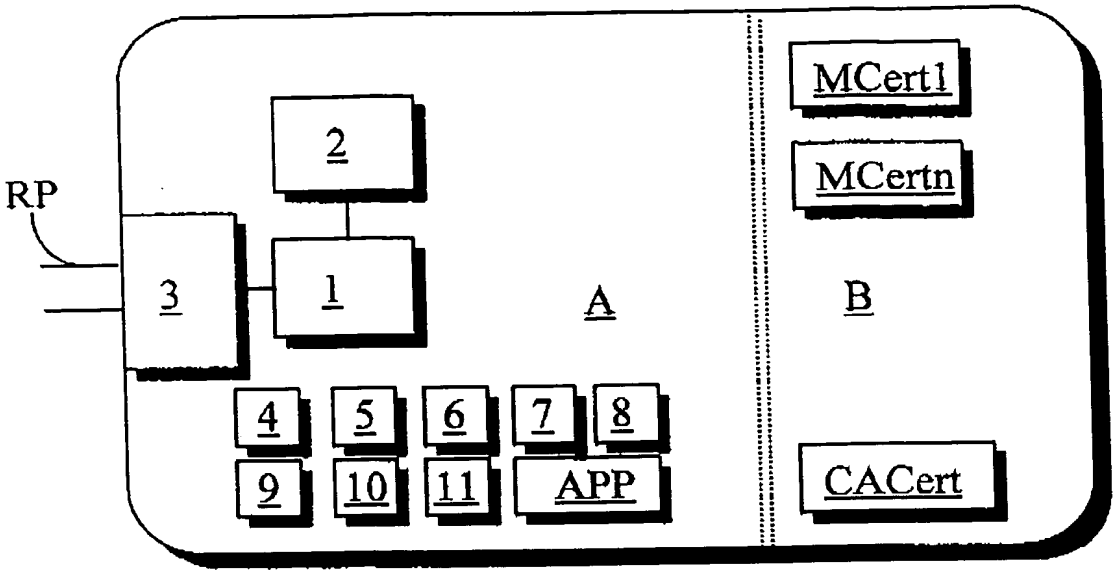

MCert1
MCertn
2
RP
3
1
A
B
4
5
6
7
8
9
10
11
APP
CACert

Fig. 1

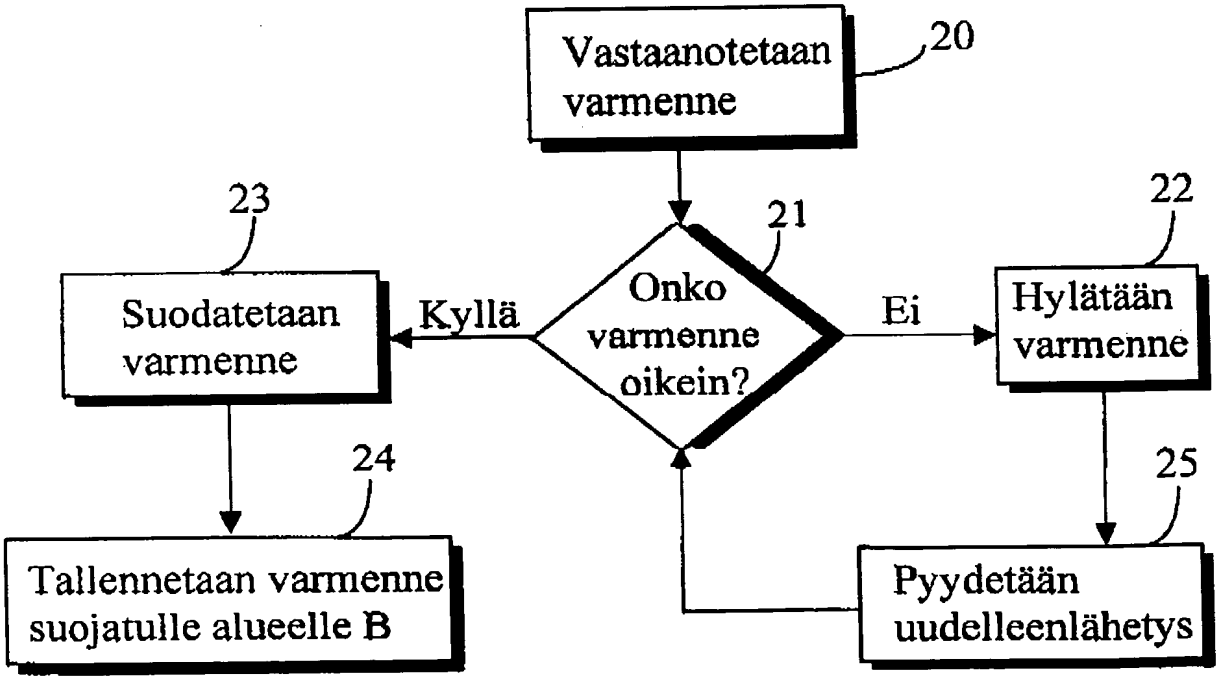
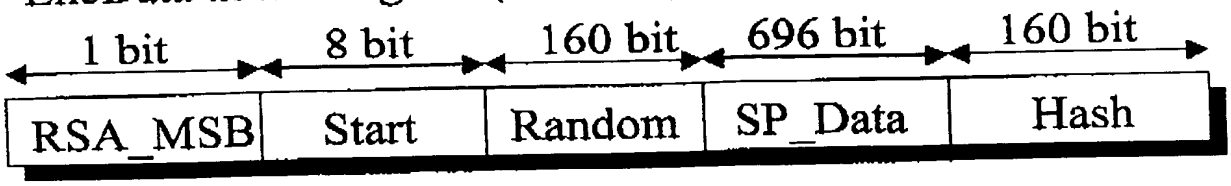
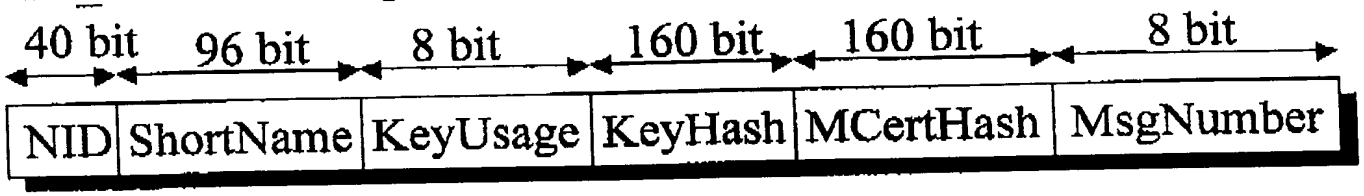

Vastaanotetaan varmenne
20
23
21
22
Suodatetaan varmenne
Kyllä
Onko varmenne oikein?
Ei
Hylätään varmenne
24
25
Tallennetaan varmenne suojatulle alueelle B
Pyydetään uudelleenlähetys

Fig. 2

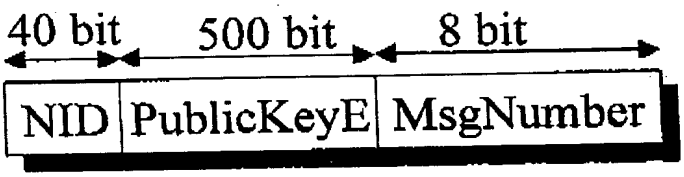
EncData in message#2 (1025 bit)



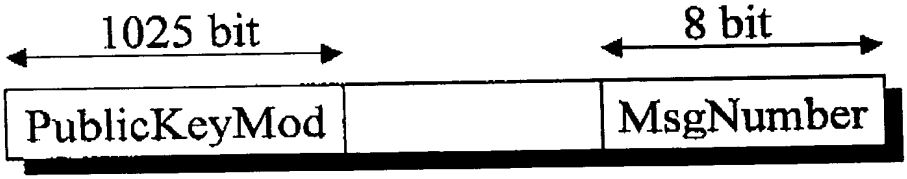

SP_Data in message#2 (696 bit)




SP_Data in message#3 (548 bit)




Non encrypted SMS-message#1




Downloaded Data in message#2

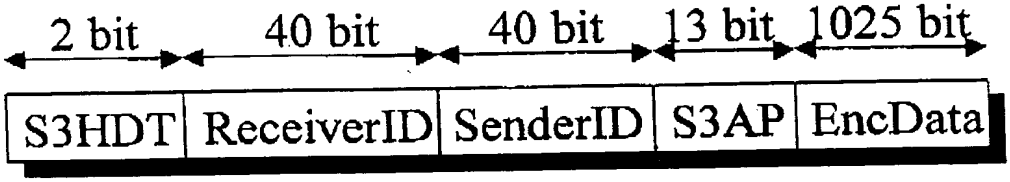



Fig. 3